

Frequently Asked Questions on Geolocation and the GPS Act

- **What is geolocation information?** Geolocation data is information generated by electronic devices – including cell phones, Wi-Fi equipped laptops, and GPS navigation units – that can be used to determine the location of these devices and the devices' owners.
- **Who uses geolocation information and how?** Geolocation information is used by a variety of companies for legitimate commercial reasons. Cell phone service providers use it to route calls to their customers, GPS navigation services use it to help their customers avoid getting lost, and a variety of technology companies use it to provide assorted online services.
- **What laws govern how geolocation data is accessed and used?** Laws pertaining to geolocation have not kept pace with technology. Judges in different jurisdictions have issued conflicting rulings about what procedures law enforcement must follow – and how much evidence is necessary – to obtain individuals' geolocation data from private companies. This lack of clarity creates problems for law enforcement agencies and private companies, as well as uncertainty for customers.
- **What does the GPS Act do?** The GPS Act establishes a clear, uniform standard for government access to geolocation data. This will give prosecutors and law enforcement officers clarity about how much evidence they need to remotely track individuals' movements. It will also give private companies clarity about when they can respond to legitimate law enforcement requests, and what obligations they have to protect their customers' information. And it will give ordinary citizens confidence that both public safety and their privacy rights are being appropriately protected.
- **How does the GPS Act work?** The GPS Act is modeled primarily after federal wiretapping statutes. This approach is based on the view that surreptitiously turning an individual's cell phone into a tracking device without their knowledge has a substantial privacy impact, just like tapping that person's phone or searching that person's house. So the GPS Act creates a process whereby government agencies can get a probable cause warrant to obtain geolocation information in the same way that they currently get warrants for wiretaps or other types of electronic surveillance.
- **How will the GPS Act impact law enforcement?** The current lack of legal clarity regarding geolocation makes it harder for law enforcement officers to do their jobs. Because the law is being interpreted differently in different jurisdictions, government agencies have to spend significant time and resources figuring out which rules apply in which situations. And government attorneys can be put in the position of having to request a court order without knowing what standards or procedures the judge expects them to follow. The GPS Act would end this confusion by providing strong, clear rules that law enforcement can confidently adhere to.

- **When would law enforcement have to get a warrant to access geolocation data?** The GPS Act would require law enforcement agencies to get a warrant when they want to acquire an individual's geolocation information from a private company. It would also require warrants when law enforcement agencies want to monitor individuals' movements directly, using covertly installed tracking devices or similar means. In emergency situations it would allow law enforcement officers to obtain the information that they need immediately and then get a warrant for their actions later.
- **When wouldn't law enforcement have to get a warrant to access geolocation data?** The legislation includes several exceptions to the warrant requirement. Warrants would not be required in cases where the individual being tracked is reasonably believed to be in danger or has requested assistance, cases where an individual's geolocation information is publicly available, cases where a mobile electronic device has been stolen, and cases where an individual (or their parent/guardian in the case of minors) has consented to being monitored.
- **Law enforcement agencies do not need a warrant to watch someone walk down the street, so why should they get a warrant to track individuals' movements electronically?** Tracking an individual's movements on twenty-four hour basis for an extended period of time is qualitatively different than visually observing that person during a single trip, and can reveal significantly more information about their activities and pattern of life. Additionally, tracking an individual with a GPS device or by tracking their cell phone is much cheaper and easier than tracking them with a surveillance team, so the resource barriers that act as a check against abuse of visual surveillance techniques do not always apply to geolocation tracking and other electronic surveillance methods.
- **Will the GPS Act impact intelligence agencies' authorities?** Existing intelligence surveillance laws do not directly address geolocation, but the GPS Act does not modify intelligence agencies' authorities to conduct electronic surveillance.
- **How will the GPS Act impact private companies?** The various commercial service providers that hold information on their customers' locations are often caught in the untenable position of having unclear and potentially conflicting obligations to both their customers and law enforcement agencies. Creating a strong legal framework to govern access to geolocation will give these companies the clarity they need to both comply with legitimate government requests and uphold their commitments to protect customers' privacy.
- **Will the GPS Act allow cell phone companies to store and sell their customers' location data?** The GPS Act permits service providers to collect geolocation information in the normal course of business, but makes it clear that these companies are only allowed to share or sell customers' data with the consent of individual customers.
- **Will smart phone apps still be allowed to access a user's location?** Yes, if the customer has given consent for his or her geolocation information to be shared for these purposes.

- **Will the GPS Act apply to anyone besides government agencies and service providers?** Yes. The GPS Act creates criminal penalties for surreptitiously using an electronic device to track a person's movements that parallel the penalties that exist for illegal wiretapping. As an example, if a woman's ex-husband taps her phone he is breaking the law. This legislation would treat hacking her GPS navigation unit to track her movements as a similar offense.
- **How will the GPS Act protect average Americans?** The GPS Act will protect average Americans' safety by giving law enforcement agencies more clarity about when they can obtain geolocation information. And it will protect their privacy rights by requiring law enforcement agencies and private companies to either get a warrant or get consent before covertly monitoring their movements on a 24/7 basis.
- **How is the GPS Act different from other legislation that has been proposed to address these issues?** There have been other worthwhile legislative solutions proposed to address the lack of legal clarity regarding geolocation, but the GPS Act is distinctive for its comprehensive approach to the problem. The GPS Act establishes clear rules for both law enforcement agencies and private entities that have access to geolocation information -- rather than only covering one or the other -- and it covers both real-time tracking and access to records of individuals' past movements in the same way.